AMENDMENTS TO THE CLAIMS

1. (Currently amended) In a system comprising at least one application and a framework, a method performed by the framework comprising:

receiving a request from the application for a customized implementation of a service;

determining a set of zero or more restrictions to be imposed upon said customized implementation;

dynamically constructing said customized implementation, said customized implementation incorporating said restrictions, and comprising enforcement logic for enforcing said restrictions; and

providing said customized implementation to the application;

wherein said customized implementation is invocable by the application without further interaction with the framework.

2. (Cancelled)

3. (Original) The method of claim 1, wherein the system further comprises a general implementation for said service, wherein said general implementation is unrestricted, and wherein said customized implementation further incorporates said general implementation.

4. (Original) The method of claim 3, wherein said enforcement logic enforces said restrictions on said general implementation.

5. (Original) The method of claim 1, wherein said enforcement logic is invoked upon initialization of said customized implementation.

6. (Original) The method of claim 5, wherein said enforcement logic, when invoked:

receives a set of desired parameters from the application;

determines whether the desired parameters exceed said restrictions; and

in response to a determination that the desired parameters exceed said restrictions, preventing said customized implementation from operating.

7. (Original) The method of claim 5, wherein said service is an encryption/decryption service, and wherein said enforcement logic, when invoked:

determines whether a particular exemption mechanism has been invoked; and

in response to a determination that the particular exemption mechanism has not been invoked, preventing said customized implementation from operating.

8. (Original) The method of claim 1, wherein determining the set of zero or more restrictions comprises:

accessing information specifying one or more limitations; and

processing said limitations to derive said restrictions.

9. (Original) The method of claim 8, wherein said service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations.

10. (Original) The method of claim 9, wherein said default encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

11. (Original) The method of claim 1, wherein determining the set of zero or more restrictions comprises:

accessing information specifying one or more limitations;

determining permissions, if any, granted to the application; and

reconciling said limitations and said permissions to derive said restrictions.

12. (Original) The method of claim 11, wherein said limitations and said permissions are reconciled to derive restrictions which are least restrictive.

13. (Original) The method of claim 11, wherein said service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations, and a set of zero or more exempt encryption limitations which apply when one or more exemption mechanisms are implemented.

14. (Original) The method of claim 13, wherein said default encryption limitations and said exempt encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

15. (Original) The method of claim 13, wherein reconciling said limitations and said permissions comprises:

determining whether the application has been granted any permissions; and

in response to a determination that the application has not been granted any permissions, deriving said restrictions from said set of default encryption limitations.

16. (Original) The method of claim 13, wherein reconciling said limitations and said permissions comprises:

determining whether the application has been granted any permissions which require implementation of a particular exemption mechanism;

in response to a determination that the application has been granted a permission which requires implementation of a particular exemption mechanism, determining whether said exempt encryption limitations allow said particular exemption mechanism to be implemented; and

in response to a determination that said exempt encryption limitations allow said particular exemption mechanism to be implemented, deriving said restrictions from said set of exempt encryption limitations.

17. (Original) The method of claim 1, wherein the system further comprises a general implementation for said service, and wherein dynamically constructing said customized implementation comprises:

instantiating the general implementation to give rise to a general implementation instance;

instantiating a wrapper object; and

encapsulating said general implementation instance and said restrictions within said wrapper object to derive said customized implementation.

18. (Original) The method of claim 17, wherein said wrapper object comprises one or more invocable methods, wherein said general implementation instance comprises one or more invocable methods, and wherein encapsulating comprises:

mapping one or more of the invocable methods of said wrapper object to one or more of the invocable methods of said general implementation instance.

19. (Original) The method of claim 18, wherein said wrapper object comprises initialization logic for enforcing said restrictions on said general implementation instance.

20. (Original) The method of claim 19, wherein said initialization logic is invoked prior to allowing any of the invocable methods of said general implementation instance to be invoked.

21. (Original) The method of claim 17, further comprising:

instantiating an exemption mechanism to give rise to an exemption mechanism instance; and

encapsulating said exemption mechanism instance within said wrapper object.

22. (Currently amended) In a system comprising at least one application, a framework comprising:

a mechanism for receiving a request from the application for a customized implementation of a service;

a mechanism for determining a set of zero or more restrictions to be imposed upon said customized implementation;

a mechanism for dynamically constructing said customized implementation, said customized implementation incorporating said restrictions, and comprising enforcement logic for enforcing said restrictions; and

a mechanism for providing said customized implementation to the application;

wherein said customized implementation is invocable by the application without further interaction with the framework.

23. (Cancelled)

24. (Original) The framework of claim 22, wherein the system further comprises a general implementation for said service, wherein said general implementation is unrestricted, and wherein the mechanism for dynamically constructing said customized implementation further incorporates said general implementation within said customized implementation.

25. (Original) The framework of claim 24, wherein said enforcement logic enforces said restrictions on said general implementation.

26. (Original) The framework of claim 22, wherein said enforcement logic is invoked upon initialization of said customized implementation.

27. (Original) The framework of claim 26, wherein said enforcement logic, when invoked:

receives a set of desired parameters from the application;

determines whether the desired parameters exceed said restrictions; and

in response to a determination that the desired parameters exceed said restrictions, preventing said customized implementation from operating.

28. (Original) The framework of claim 26, wherein said service is an encryption/decryption service, and wherein said enforcement logic, when invoked:

determines whether a particular exemption mechanism has been invoked; and

in response to a determination that the particular exemption mechanism has not been invoked, preventing said customized implementation from operating.

29. (Original) The framework of claim 22, wherein the mechanism for determining the set of zero or more restrictions comprises:

a mechanism for accessing information specifying one or more limitations; and

a mechanism for processing said limitations to derive said restrictions.

30. (Original) The framework of claim 29, wherein said service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations.

31. (Original) The framework of claim 30, wherein said default encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

32. (Original) The framework of claim 22, wherein the mechanism for determining the set of zero or more restrictions comprises:

a mechanism for accessing information specifying one or more limitations;

a mechanism for determining permissions, if any, granted to the application; and

a mechanism for reconciling said limitations and said permissions to derive said restrictions.

33. (Original) The framework of claim 32, wherein said limitations and said permissions are reconciled to derive restrictions which are least restrictive.

34. (Original) The framework of claim 32, wherein said service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations, and a set of zero or more exempt encryption limitations which apply when one or more exemption mechanisms are implemented.

35. (Original) The framework of claim 34, wherein said default encryption limitations and said exempt encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

36. (Original) The framework of claim 34, wherein the mechanism for reconciling said limitations and said permissions comprises:

a mechanism for determining whether the application has been granted any permissions; and

a mechanism for deriving, in response to a determination that the application has not been granted any permissions, said restrictions from said set of default encryption limitations.

37. (Original) The framework of claim 34, wherein the mechanism for reconciling said limitations and said permissions comprises:

a mechanism for determining whether the application has been granted any permissions which require implementation of a particular exemption mechanism;

a mechanism for determining, in response to a determination that the application has been granted a permission which requires implementation of a particular exemption mechanism, whether said exempt encryption limitations allow said particular exemption mechanism to be implemented; and

a mechanism for deriving, in response to a determination that said exempt encryption limitations allow said particular exemption mechanism to be implemented, said restrictions from said set of exempt encryption limitations.

38. (Original) The framework of claim 22, wherein the system further comprises a general implementation for said service, and wherein the mechanism for dynamically constructing said customized implementation comprises:

a mechanism for instantiating the general implementation to give rise to a general implementation instance;

a mechanism for instantiating a wrapper object; and

a mechanism for encapsulating said general implementation instance and said restrictions within said wrapper object to derive said customized implementation.

39. (Original) The framework of claim 38, wherein said wrapper object comprises one or more invocable methods, wherein said general implementation instance comprises one or more invocable methods, and wherein the mechanism for encapsulating comprises:

a mechanism for mapping one or more of the invocable methods of said wrapper object to one or more of the invocable methods of said general implementation instance.

40. (Original) The framework of claim 39, wherein said wrapper object comprises initialization logic for enforcing said restrictions on said general implementation instance.

41. (Original) The framework of claim 40, wherein said initialization logic is invoked prior to allowing any of the invocable methods of said general implementation instance to be invoked.

42. (Original) The framework of claim 38, further comprising:

a mechanism for instantiating an exemption mechanism to give rise to an exemption mechanism instance; and

a mechanism for encapsulating said exemption mechanism instance within said wrapper object.

43. (Currently amended) In a system comprising at least one application, a computer readable medium having stored thereon instructions which, when executed by one or more processors, cause the one or more processors to implement a framework which dynamically constructs a customized implementation of a service, said computer readable medium comprising:

instructions for causing one or more processors to receive a request from the application for a customized implementation of a service;

instructions for causing one or more processors to determine a set of zero or more restrictions to be imposed upon said customized implementation;

instructions for causing one or more processors to dynamically construct said customized implementation, said customized implementation incorporating said restrictions, and comprising enforcement logic for enforcing said restrictions; and

instructions for causing one or more processors to provide said customized implementation to the application;

wherein said customized implementation is invocable by the application without further interaction with the framework.

44. (Canceled)

45. (Original) The computer readable medium of claim 43, wherein the system further comprises a general implementation for said service, wherein said general implementation is unrestricted, and wherein said customized implementation further incorporates said general implementation.

46. (Original) The computer readable medium of claim 45, wherein said enforcement logic enforces said restrictions on said general implementation.

47. (Original) The computer readable medium of claim 43, wherein said enforcement logic is invoked upon initialization of said customized implementation.

48. (Original) The computer readable medium of claim 47, wherein said enforcement logic, when invoked:

receives a set of desired parameters from the application;

determines whether the desired parameters exceed said restrictions; and

in response to a determination that the desired parameters exceed said restrictions, preventing said customized implementation from operating.

49. (Original) The computer readable medium of claim 47, wherein said service is an encryption/decryption service, and wherein said enforcement logic, when invoked:

determines whether a particular exemption mechanism has been invoked; and

in response to a determination that the particular exemption mechanism has not been invoked, preventing said customized implementation from operating.

50. (Original) The computer readable medium of claim 43, wherein the instructions for causing one or more processors to determine the set of zero or more restrictions comprises:

instructions for causing one or more processors to access information specifying one or more limitations; and

instructions for causing one or more processors to process said limitations to derive said restrictions.

51. (Original) The computer readable medium of claim 50, wherein said service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations.

52. (Original) The computer readable medium of claim 51, wherein said default encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

53. (Original) The computer readable medium of claim 43, wherein the instructions for causing one or more processors to determine the set of zero or more restrictions comprises:

instructions for causing one or more processors to access information specifying one or more limitations;

instructions for causing one or more processors to determine permissions, if any, granted to the application; and

instructions for causing one or more processors to reconcile said limitations and said permissions to derive said restrictions.

54. (Original) The computer readable medium of claim 53, wherein said limitations and said permissions are reconciled to derive restrictions which are least restrictive.

55. (Original) The computer readable medium of claim 53, wherein said service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations, and a set of zero or more exempt encryption limitations which apply when one or more exemption mechanisms are implemented.

56. (Original) The computer readable medium of claim 55, wherein said default encryption limitations and said exempt encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

57. (Original) The computer readable medium of claim 55, wherein the instructions for causing one or more processors to reconcile said limitations and said permissions comprises:

instructions for causing one or more processors to determine whether the application has been granted any permissions; and

instructions for causing one or more processors to derive, in response to a determination that the application has not been granted any permissions, said restrictions from said set of default encryption limitations.

58. (Original) The computer readable medium of claim 55, wherein the instructions for causing one or more processors to reconcile said limitations and said permissions comprises:

instructions for causing one or more processors to determine whether the application has been granted any permissions which require implementation of a particular exemption mechanism;

instructions for causing one or more processors to determine, in response to a determination that the application has been granted a permission which requires implementation of a particular exemption mechanism, whether said exempt encryption limitations allow said particular exemption mechanism to be implemented; and

instructions for causing one or more processors to derive, in response to a determination that said exempt encryption limitations allow said particular exemption mechanism to be implemented, said restrictions from said set of exempt encryption limitations.

59. (Original) The computer readable medium of claim 43, wherein the system further comprises a general implementation for said service, and wherein the instructions for causing one or more processors to dynamically construct said customized implementation comprises:

instructions for causing one or more processors to instantiate the general implementation to give rise to a general implementation instance;

instructions for causing one or more processors to instantiate a wrapper object; and

instructions for causing one or more processors to encapsulate said general implementation instance and said restrictions within said wrapper object to derive said customized implementation.

60. (Original) The computer readable medium of claim 59, wherein said wrapper object comprises one or more invocable methods, wherein said general implementation instance comprises one or more invocable methods, and wherein the instructions for causing one or more processors to encapsulate comprises:

instructions for causing one or more processors to map one or more of the invocable methods of said wrapper object to one or more of the invocable methods of said general implementation instance.

61. (Original) The computer readable medium of claim 60, wherein said wrapper object comprises initialization logic for enforcing said restrictions on said general implementation instance.

62. (Original) The computer readable medium of claim 61, wherein said initialization logic is invoked prior to allowing any of the invocable methods of said general implementation instance to be invoked.

63. (Original) The computer readable medium of claim 59, further comprising:

instructions for causing one or more processors to instantiate an exemption mechanism to give rise to an exemption mechanism instance; and

instructions for causing one or more processors to encapsulate said exemption mechanism instance within said wrapper object.

64. (New) The method of claim 1, wherein said framework comprises Java Cryptography Extension to Java Platform.

65. (New) The framework of claim 22, wherein said framework comprises Java Cryptography Extension to Java Platform.

66. (New) The computer readable medium of claim 43, wherein said framework comprises Java Cryptography Extension to Java Platform.